JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718

VOLUME . 4 ISSUE . 2 (2025)

IDENTITY THEFT RISK ASSESSMENT TOOLS IN THE BANKING SECTOR OF PAKISTAN

Amna Abro
Institute of computer Science, Shah Abdul Latif University, Khairpur Mir's
abdullah.maitlo@salu.edu.pk
Abdullah Maitlo
Institute of computer Science, Shah Abdul Latif University, Khairpur Mir's
abroamna5@gmail.com
Mumtaz Hussain Mahar
Department of Computer Science, SZABIST University, Larkana Campus
mumtaz.mahar@lrk.szabist.edu.pk

RECEIVED	ACCEPTED	PUBLISHED
02 July 2025	15 July 2025	6 Aug 2025

ABSTRACT
Identity theft has emerged as a critical threat to the financial security of customers and the integrity of banking operations in Pakistan. With increasing digitization of financial services, banks face mounting risks related to fraudulent access, impersonation, and unauthorized data usage. This research investigates the effectiveness of existing risk assessment tools implemented by banks in Pakistan for detecting and preventing identity theft. By analyzing security practices, technologies used, and challenges faced by banking institutions, this study highlights gaps in risk assessment mechanisms and proposes an improved model based on global best practices. The findings contribute to building a more resilient banking infrastructure capable of proactively managing identity-related fraud.

Keywords. Identity Theft, Risk Assessment Tools, Banking Sector, Cyber Security, Case Study, Qualitative Study

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

Introduction

Digital banking has revolutionized financial services globally, and Pakistan is no exception. As the central bank of Pakistan, the State Bank continues to develop the digital transformation environment along with its initiatives, such as Raast or branchless banking guidelines, millions of customers have access to convenient and real-time financial services. However, this digital expansion also introduces unprecedented cybersecurity risks, with identity theft emerging as one of the most pressing threats to customer trust and institutional security. The process of identity theft in the banking industry implies unauthorized access to personal or financial data of a person to subsequently use it to implement various fraudulent actions, including unauthorized transactions, secured loans, account hijacking, etc. In Pakistan the social engineering, phishing scams and loopholes in legacy verification systems have all been used as avenues by the criminal geniuses to exploit identity theft in an increasingly sophisticated manner.

Even though such regulatory authorities as the State Bank of Pakistan and NADRA have initiated action to enforce e-KYC (electronic Know Your Customer) procedures, introduce biometric verification, and require the auditing of cybersecurity, the efficiency of such practices varies greatly between the types of banks. The banks in the public sector commonly have poor systems and low budgets, private and Islamic banks are still at different phases of using modern identity risk solutions, including AI-based fraud prevention and behavioral biometrics. Given this backdrop, it becomes essential to understand how banks in Pakistan are addressing the risk of identity theft. This paper will also attempt to establish a comparison between the identity theft risk assessment tools utilized in the three predominant categories of banks in Pakistan-namely private-sector bank, public-sector bank and the Islamic bank. The studied research helps to understand the issues of institutional preparedness, technology adoption, and policy implementation in the battle against identity theft through the multiple-case study that involves a qualitative research design.

2. Research Objectives

To explore the identity theft risk assessment practices in Pakistani banks.

To compare the implementation of these tools across different banking institutions.

To identify key barriers and enablers in deploying effective risk assessment mechanisms.

3. Literature Review

3.1 Introduction

Identity theft is a persistent and evolving threat in the digital financial landscape. It consists of diversion of personally identifiable information (PII) and its improper use without the authorization of the owner to engage in impersonation, most often in the commission of fraudulent financial activity. As the banking has gone digital especially in developing nations such as Pakistan, the threat to identity theft has been getting high. The given literature review summarizes global and local understanding of the identity theft, analyzes risk audit tools and technologies and speaks about the particular regulatory, institutional and technological environment of the Pakistani banking market.

3.2 Global Perspectives on Identity Theft in Banking

In the world, the financial sector has been one of the most popular spheres which are exposed to identity theft because security services in this field have access to personal and financial data. According to Anderson et al. (2021), identity theft has been a sophisticated crime, which requires the use of several methods, including phishing, malware, and social engineering. To reflect this reality, institutions have developed different risk assessment models to include the NIST Cybersecurity Framework (2018), ISO/IEC 27001 framework and the GDPR compliant identity verification systems. The emergence of digital and mobile banking has

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

brought about the problem of new identity verification. Smith and Lacey (2022) emphasize that the use of traditional statistic verification, such as passwords and PINs is no longer enough. Data breaches and credential stuffing that are typically used in modern identity theft can bypass these security measures. Financial institutions are therefore spending in dynamic, real-time tools that involve behavioral biometrics, Artificial Intelligence algorithms and multiple-factor authentication to evaluate the risk.

3.3 Risk Assessment Frameworks and Tools

Management of identity theft includes risk assessment, which is a process of assessing threats, vulnerabilities and how much they affect it. The tools go all the way down to manual checklists and audit processes and up to state of the art AI powered engines. ISO/IEC 27005 standard provides a step by step guidance on how information security risk management should be carried out comprising identification, analysis, evaluation and remedial processes. A meta-analysis by Zhao and Lee (2021) produced strong results that show machine learning methods in identity risk scoring are incredibly effective to predict fraudulent behavior on historical and real-time data. Behavioral analytics software is able to identify user-device abnormalities including log-in, geographical location, amount transacted, and device fingerprint. These abnormal exceptions transgressing the known better practices are either identified as requiring direct inspection or simply blocked. Supervised learning and neural networks employing AI-based solutions to detect synthetic identity fraud is particularly applicable in the light of irregularities developed through real and false information amalgamated to make up a new fake identity. The tools also facilitate continuous monitoring that is a major differentiator to older rule based systems which only evaluated risk at logons or transaction points.

3.4 Pakistani Context: Cybersecurity and Identity Theft

Digital banking has become prevalent in Pakistan as regulatory overtures led to its swift absorption. The report by the State Bank of Pakistan (2023) revealed that mobile banking resources were accessed by more than 20 million users in the year 2022, which was a 30 percent improvement compared to the year 2021. It is with this development though that there is a rise in cyber threats. Iqbal et al. (2024) highlight that identity theft is one of the top three cybersecurity concerns among financial institutions in Pakistan. Pakistan's digital ecosystem is supported by NADRA, which maintains the country's biometric and demographic data. Many banks now use NADRA's APIs for biometric verification during account opening. Despite this integration, challenges persist in using identity verification throughout the customer lifecycle. Rehman et al. (2023) argue that many banks, especially public-sector institutions, only use identity verification during onboarding, missing the opportunity to monitor transactions and sessions for ongoing fraud. Abbas and Arif (2022) explored customer perceptions of cybersecurity in Pakistani banks and found a strong correlation between perceived security and willingness to adopt digital banking. However, awareness of identity theft among users remains low, and banks do not consistently educate customers on how to protect their personal information.

3.5 Biometric and Behavioral Identity Tools

Biometric authentication is increasingly adopted in Pakistan's banking sector. UBL, HBL, and Meezan Bank are among the early adopters of fingerprint and facial recognition tools for user login and transaction approval. These technologies offer a higher degree of security compared to traditional credentials. However, biometric systems are not foolproof—spoofing attacks and biometric data breaches can still occur. Behavioral biometrics, such as typing patterns, mouse dynamics, and app navigation behavior, are emerging as tools to assess identity risk in a non-intrusive manner. Khan and Farooq (2023) highlight that these methods are under pilot testing in several Pakistani banks and could offer continuous authentication without disrupting the user experience. However,

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

implementation remains limited due to infrastructure costs and lack of skilled personnel.

3.6 Ethical and Regulatory Considerations

The State Bank of Pakistan has issued various guidelines under its cybersecurity framework, mandating periodic audits, customer due diligence, and secure digital onboarding. Islamic banks face additional ethical considerations in using AI tools for identity profiling. Bank C in this study, for instance, refrains from implementing aggressive profiling algorithms that could lead to discrimination or breach of privacy, aligning with Shariah principles. Regulatory compliance remains inconsistent. While top-tier private banks follow SBP regulations strictly, smaller or regional banks struggle with implementation due to lack of resources. Business Recorder (2024) reported that even among banks that have implemented biometric tools, there are discrepancies in data storage, encryption standards, and customer consent mechanisms.

Although studies based on quantification have been conducted on the cases of identity theft and customer habits, there is also the absence of a qualitative research that looks at how these institutions arrive at decisions on identity risk management. There is a limited case study put on individual institutions particularly those in developing countries. This paper fills this research gap by researching upon the views and management of identity theft risk by three types of banks in Pakistan which include private, public, and Islamic banks. The multi-case research method delivers a better understanding of the institutional behavior, cultural and ethical issues, and practical constraints that are usually not considered in quantitative constructs. It is also instrumented to serve the increasing literature super-set which seeks localized cybersecurity support that is context-conscious with South Asia being one such location. The literature emphasizes that identity theft is a dynamic threat requiring adaptive, technology-driven responses. Although international experiences serve as a blueprint on how to achieve the security of digital banking, local strategies are necessary. The banking industry in Pakistan has shown both proactive and reactive responses, wherein the process of innovation can be prompted by the presence of the private banks. Nevertheless, a distinct set of limitations is proposed by public-sector and Islamic banks and have to be addressed accordingly. This research builds on these insights by presenting comparative qualitative evidence from the field, bridging the knowledge gap between global frameworks and local realities.

4. Research Methodology

This research employs a qualitative multiple-case study approach to examine how three different types of banks in Pakistan manage identity theft risk. The banks include the public, private sector and the Islamic bank area. The methodological approach leans on the principles of the case study design provided by Yin (2018) and is based on a triangulated set of data sources that would allow obtaining a deeper contextual picture. Three case studies were conducted in three different banks of Pakistan. The banks were name Bank A, Bank B and Bank C. the banks were selected after consideration of Technologically advanced with a robust cybersecurity team, limited IT infrastructure and digital maturity and ethically cautious in use of AI and analytics.

The data Collection methods included one to one semi structured interviews, document analysis and participant observation. In total 32 interviews were conducted with cybersecurity officers, compliance officers, digital banking staff, and risk analysts. Document analysis included internal risk reports, SBP audit results, and KYC procedures and participant observations included real-time onboarding and transaction handling in branches and digital platforms. Whereas, data analyzed using thematic analysis (Braun & Clarke, 2006) using NVivo software identified patterns in identity theft risk assessment strategies, challenges, and organizational culture. Codes were developed both inductively and deductively. A complete ethical consideration institutional anonymity was maintained. Interviews were conducted with informed consent. Sensitive data were handled in encrypted storage systems. Religious and cultural sensitivities at all Banks

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

were respected in both data collection and analysis.

5. Findings

This section presents the findings of the study based on 32 in-depth interviews, document analysis, and observations conducted across three major banks in Pakistan—Bank A, Bank B, and Bank C. The findings are structured by individual case studies, followed by a comparative cross-case analysis.

5.1 Case Study: Bank A

Bank A is a top-tier commercial bank in Pakistan known for its innovation in digital banking and its proactive adoption of cybersecurity tools. The bank has made significant investments in AI-driven fraud detection, real-time monitoring systems, and advanced identity verification mechanisms.

5.1.1. Identity Verification and Risk Assessment Tools

Bank A integrates biometric authentication (fingerprint and facial recognition) with NADRA's national identity database for customer onboarding and digital banking services. Additionally, it employs behavioral biometrics, analyzing typing speed, mouse movements, navigation behavior, device fingerprinting, and geolocation to assess identity in real-time. The bank uses dynamic identity scoring models that continuously monitor user sessions and assign a risk score. If anomalies are detected—such as a login from an unusual location or a sudden change in transaction patterns—the system triggers multi-factor authentication or temporarily blocks access until verification is completed.

5.1.2. AI-Driven Analytics

The AI models are trained using supervised learning on historical fraud datasets. These models are capable of detecting emerging fraud patterns, such as synthetic identities, mule accounts, and deepfake attempts. Interviewees emphasized that the models are regularly retrained to reduce false positives and adjust to evolving cyber threats.

5.1.3. Operational Capabilities and Staff Readiness

A dedicated fraud detection and cybersecurity team operates a Security Operations Center (SOC), which functions 24/7. Staff undergo continuous professional development and are required to pass internal certifications on information security. Bank A also collaborates with external consultants for red-teaming exercises and vulnerability assessments.

5.1.4. Customer Education and Communication

Bank A actively educates its customers through SMS alerts, email campaigns, digital tutorials, and social media engagement. There are regular webinars and in-app messages that inform users about phishing, safe password practices, and the risks of identity theft. Despite this, some interviewees admitted that older and rural customers are still vulnerable due to low digital literacy.

5.1.5. Challenges Identified

False positives from behavioral analysis often inconvenience legitimate users.

Biometric systems sometimes fail in low-bandwidth areas or with elderly users.

AI models may reflect biases due to underrepresented user groups in training data.

5.2 Case Study: Bank B

Bank B is a large, government-owned institution that serves a wide demographic, especially in rural and low-income areas. While it has introduced some digital banking features, its infrastructure and risk assessment systems are significantly underdeveloped.

5.2.1. Identity Verification Practices

Customer verification relies heavily on physical CNIC checks and manual procedures. NADRA integration is limited to a few urban branches, with frequent system outages reported. There is no biometric login or continuous session monitoring in place. Identity theft risk is assessed reactively rather than proactively. Fraudulent activity is often only detected after a customer complaint is lodged or a loss has occurred.

5.2.2. Operational Limitations

Interviews with staff revealed severe under-resourcing of the IT and cybersecurity departments. The bank lacks the personnel and

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

budget to implement modern identity risk tools. Internal fraud response is slow due to outdated systems and cumbersome communication between departments. The fraud detection team reviews cases manually and often work with outdated log files or incomplete transaction histories.

5.2.3. Training and Awareness

Training in digital risk and identity verification is sporadic and inconsistent. Most front-line staff have limited knowledge of cybersecurity best practices. Customers are seldom educated about digital fraud risks unless a breach has occurred. Many employees described compliance as a "paper exercise," driven more by audit requirements than internal motivation for risk mitigation.

5.2.4. Challenges Identified

- Absence of real-time monitoring systems.
- Minimal investment in cybersecurity infrastructure.
- Bureaucratic constraints on technology procurement and policy reform.
- Lack of skilled cybersecurity personnel and continuous training mechanisms.

5.3 Case Study: Bank C

Bank C operates under Shariah principles and adopts a cautious approach to identity risk management. It maintains a balance between adopting digital solutions and adhering to ethical and religious norms that discourage intrusive surveillance or profiling.

5.3.1. Verification Methods

Bank C uses biometric verification during account creation and for high-value transactions. It has integrated with NADRA for identity confirmation but avoids using profiling algorithms that assess users based on income, gender, or demographic patterns. The bank emphasizes consent-based data handling. Customers are required to explicitly agree to data usage policies, and the bank avoids aggressive data mining practices.

5.3.2. Ethical Boundaries in AI Use

Bank C has limited adoption of AI in fraud detection. While some rule-based systems are in place for basic anomaly detection, the bank refrains from using neural networks or probabilistic scoring models due to concerns about transparency and accountability. Manual review processes are prioritized. Suspected identity theft cases are escalated to human fraud analysts, who use internal protocols and consult with compliance teams to make decisions.

5.3.3. Staff and Ethical Oversight

The bank's Shariah board oversees the design of digital systems to ensure alignment with Islamic ethics. Interviewees explained that the board has rejected certain tools that rely on customer surveillance or predictive modeling, citing risks of discrimination or privacy violation. There is a dedicated ethics officer who works with the IT and compliance teams to review proposed identity verification technologies.

5.3.4. Customer Education and Awareness

Customer communication is conservative. The bank uses in-branch consultations, brochures, and SMS messages to inform users. There is no behavioral alert system in place on the mobile app or internet banking platform.

5.3.5. Challenges Identified

Delayed fraud detection due to lack of automation.
Shortage of staff trained in both AI and Islamic jurisprudence.
Difficulty in scaling ethical practices to digital environments.
Hesitation to adopt profiling-based or surveillance-intensive technologies.

6. Discussion: Cross-Case Analysis

This section synthesizes the results of the three case studies - Bank A, Bank B, and Bank C - to examine how each institution approaches identity theft risk assessment. The discussion is grounded in the findings presented earlier and cross-referenced with contemporary literature on cybersecurity, banking, and identity risk management. Through thematic analysis, we explore similarities and differences across the banks in terms of technological readiness, risk perception, institutional culture, ethical considerations, regulatory interpretation, and human capital.

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

6.1 Technological Readiness and Digital Infrastructure

The role of technology is prevalent in all areas of the society (Akram et al., 2022, 2021a, 2021b, 2021c; Al-Adwan et al., 2022; Ma et al., 2024; Ramzan et al., 2025, 2023; Chen & Ramzan, 2024). Similarly, it is important in managing identity theft risk is central to modern banking, and the cases reflect stark contrasts in infrastructure maturity.

Bank A, as a leading private sector institution, has embraced real-time identity verification tools, AI-based fraud detection models, and behavioral analytics. These tools align with global best practices, such as those highlighted by Smith and Lacey (2022), who emphasize the importance of dynamic authentication in deterring identity-related fraud. The use by the bank of machine learning algorithms that learn to recognize suspicious activity over time to ensure effective identity risk management is in line with the research results of Zhao, Lee (2021), who suggest that behavioral profiling should be used to ensure effective identity risk management.

Bank B, in contrast, lags significantly. Its outdated systems rely on manual documentation and physical CNIC verification, with very limited integration with NADRA and no session monitoring. According to the literature, it represents a typical gap in the system of public-sector institutions when insufficiency of funding and stagnation of policies do not allow innovations (Rehman et al., 2023). Bank B is a typical example of a reactive approach that provides in such studies since in this case, fraud is most frequently identified ex post which leads to dissatisfaction of customers and losses.

Bank C, while technologically capable, deliberately limits its use of advanced profiling and surveillance tools due to its ethical commitments as an Islamic financial institution. The selective use of AI tools by the bank represents the issue of privacy, transparency, and implications of bias, all of which become other topics of the debate around ethical AI (Anderson et al., 2021). Although such a second strategy can undermine its operational efficiency, it increases the confidence of the customer in terms of handling of their data, especially with customers having religious inclinations.

The differences indicate that although infrastructure is very critical in the prevention of identity theft, adoption will depend more on values and institutional objectives rather than resources/capability.

6.2 Organizational Culture and Risk Perception

The perception of identity theft as a risk varies dramatically across the three institutions, influencing how aggressively they implement preventative measures.

Bank A embodies a proactive risk culture. The bank does not only consider identity verification as regulatory requirement, but as a form of competitive differentiation. The IT-based and customer-facing employees are also being trained in a routine pattern on the aspects of fraud detection and cybersecurity. This is consistent with the notion of cybersecurity maturity raised by NIST (2018) and in which risk management is so much a part and parcel of operational strategy.

Bank B, on the other hand, illustrates a compliance-driven culture. The employees perceive the risk of identity theft as an external threat instead of the weakness of the organization. Such attitude leads to the lag in responding to fraud and excessive adherence to the set of orders instead of in-house innovation. According to Iqbal et al. (2024), this behavior is typical of bureaucratic environments where change is incremental and reactive.

Bank C promotes a risk-aware yet ethically constrained culture. There is much reluctance in the utilization of such tools because the employees are driven by their religious and moral interests. This mirrors the findings of Abbas and Arif (2022), who argue that Islamic financial institutions often incorporate ethical risk filtering into technological decisions.

When considered together, the two cases support the argument that there is a necessity of context-sensitive approach towards risk culture. Readiness and willingness to implement specific measures will vary among the institutions depending on the perception and importance

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

attached to the risk that may be influenced by vision, types of clients, and structures.

6.3 Staff Expertise and Human Capital

Human capital is a critical enabler of technological solutions, yet it is unevenly distributed among the banks.

Bank A has invested in continuous professional development, including annual cybersecurity certification, red-teaming exercises, and partnerships with security consultants. Such an investment guarantees that its technology stack is complimented by competent individuals that can utilize it accordingly. Khan and Farooq (2023) point out that the best systems might be insufficiently efficient or might be potentially broken because of the lack of trained staff.

Bank B suffers from a significant skills gap. Regional, rurally-located personnel are commonly illiterate in cybersecurity, IT departments are stretched and operating using archaic systems. Such an incompatibility of operational requirement and human capability makes the bank a special target to identity thefts. Literature on digital banking in developing countries identifies such gaps as systemic challenges (Rehman et al., 2023).

Bank C faces a unique constraint: the need for dual expertise in both Islamic jurisprudence and information technology. Professionals who are knowledgeable about Shariah law and possess expertise on highly sophisticated AI systems are few hence the rate at which the bank can innovate without interfering with its ethical practice is also low.

The disparities suggest a need for sector-wide training programs and regulatory incentives to promote cybersecurity literacy. In the case of institutions with special missions or values, i.e., Islamic banks, the existing knowledge gap could be curtailed by introducing special types of certification that merged ethics, law and technology.

6.4 Regulatory Alignment and Implementation

The state bank of Pakistan (SBP) offers regulatory advice on customer due diligence, identity verification and best practices on cybersecurity. The problem is that implementation of these guidelines differs, however, yet still alters the stereotype.

Bank A goes beyond SBP requirements, incorporating third-party audits and integrating international frameworks like ISO/IEC 27005. The fact that it is in concurrence with risk models framework of NIST confirms that high compliance is possible to be in conjunction with innovation.

Bank B, while formally compliant, treats SBP guidelines as procedural necessities rather than opportunities for improvement. Issues of internal audits usually show inconsistencies in the KYC compliance and information security, which has also been reported by Business Recorder (2024). Bureaucratic inertia in the public sector can be seen as a key obstacle to uniform enforcement of regulations.

Bank C complies with SBP mandates but often negotiates exemptions or alternative measures to ensure ethical alignment. Such a two-tier system of compliance, both legal and religious, is non-existent in most parts of the world but might prove problematic during a time of crisis when the regulatory community needs to act swiftly, e.g. in case of a security incident.

The difference in regulation interpretation and implementation indicates the necessity of hyper regulation- a mode in which fundamental security requirements could be held constants but implementation could vary in line with institutional type, scale and ethical orientation.

6.5 Customer Communication and Awareness

Identity theft risk management is not only a technical issue but also a behavioral one, and customer awareness plays a vital role.

Bank A has robust customer engagement strategies, including alerts, tutorials, and awareness campaigns. This empowers users to recognize phishing attempts, avoid risky behaviors, and participate actively in their own security. These practices echo international recommendations on digital security culture (NIST, 2018).

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

Bank B largely neglects customer education. Most users are unaware of basic fraud prevention strategies. This is especially dangerous given that many of its customers are new to digital banking and may be easily deceived by social engineering attacks.

Bank C uses traditional, in-person communication such as brochures and face-to-face consultations to educate users. Although this strategy works among certain groups, it is not scalable, and prompt when threats are emerging. This crucial gap could be solved through one of the pan-nation digital literacy initiatives, bank-relevant and perhaps led and coordinated by SBP along with banks, which will minimise the exposure of identity theft in every sector.

6.6 Ethical and Cultural Dimensions

Bank C can add an element not found in most identity risk-related calculations, namely ethics and religious compliance. It refuses the use of profiling algorithms or models which rely on demographics because it worries about surveillance, discrimination and privacy, which are all subjects of Western debate on ethical AI (Anderson et al., 2021). Although technological efficiency may seem to be constrained by ethical considerations, the latter contributes to increasing customer confidence. The desire to entrust money to an institution that shares the same moral inclinations despite the delays in the transaction approval or conservative risk measurement can be common among many customers especially in faith based societies.

This ethical solution together with transparent, explainable AI may become a template of value-driven innovations not only in Islamic banks but also in the whole financial industry.

6.7 Implications for Policy and Practice

This discussion indicates that such one size fits all method of determining identity theft risk is not an effective as well as not a practically applicable method in Pakistan. The variability of institutional tasks, capabilities, and values will require a layered regulatory approach:

- **Tier 1 (High-Capacity Banks)**: Institutions like Bank A should be encouraged to innovate using full-spectrum AI tools, with clear reporting mechanisms and ethical review boards.

Tier 2 (Ethical-Constrained Banks): Institutions like Bank C should be supported in deploying context-appropriate tools, including Shariah-compliant risk assessment technologies.

Tier 3 (Resource-Constrained Banks): Financial institutions such as Bank B should have the access to the basic security tools and capacity building programs and the stricter audits at the subsidized level to help the compliance with the minimal levels.

In addition, policy frameworks have to ensure inter-bank knowledge sharing, development of cybersecurity workforce, and introduction of ethical AI certifications. Besides making the country more resilient to identity theft, such efforts would equally benefit the digital banking space in Pakistan, which is within the process of expanding. This cross-case discussion underscores the complexity of managing identity theft in a diverse banking landscape. Whereas Bank A boasts proactive, technology-oriented initiatives, Bank B is hampered by inefficiency in its system and, Bank C is focusing on ethical positions rather than aggressive automation.

The key findings of the research consist in the fact that good identity risk management needs more than technology. It entails organizational culture, moral sensitivity, human potential and regulatory flexibility. There needs to be a more suitable, collaborative effort between Banks, Regulators and Technology Developers to develop resilient and inclusive identity protection strategies in the banking industry in Pakistan.

7. Theoretical and Practical Contributions

7.1 Theoretical Contributions

The study will add to the existing literature on the same subject as there is a developing stream of identity theft, cybersecurity, and banking in developing countries literature by providing the contextual, multi-case qualitative analysis. While prior research (e.g., Zhao & Lee, 2021; Anderson et al., 2021) has largely emphasized technological innovations and quantitative modeling in identity risk assessment, this research expands the theoretical landscape in several ways:

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

7.1.1 Contextualization of Identity Theft Risk in a Developing Country

The study adds depth to global discourses by focusing on Pakistan—a developing economy with rapid digitalization but uneven institutional capacity. It responds to gaps in the literature (highlighted in section 3.7) that call for localized, qualitative investigations. The findings demonstrate how national infrastructure, digital literacy, and regulatory variability influence identity theft risk differently than in more developed countries.

7.1.2. Integration of Ethical Dimensions in Risk Assessment

The analysis of Bank C (Islamic bank) introduces a novel ethical-theoretical layer by integrating Islamic banking values into identity risk discourse. While global studies on ethical AI and cybersecurity ethics exist, few have explored how religious principles directly shape tool adoption and risk modeling. This opens up new avenues for theorizing how culture, ethics, and religion intersect with cybersecurity practices.

7.1.3. Cross-Case Risk Culture Framework

This research introduces a three-tier framework of institutional risk culture - proactive (Bank A), reactive (Bank B), and ethically cautious (Bank C) - which can inform future comparative studies. This framework provides a basis for theorizing how risk perception and organizational culture co-determine technology adoption, regulatory compliance, and user education in digital financial services.

7.1.4. Multi-Level Identity Risk Governance

The study contributes a layered understanding of identity risk governance, incorporating micro-level (user behavior), meso-level (institutional processes), and macro-level (regulatory and ethical norms). This multi-level perspective broadens traditional models that often isolate one dimension (e.g., technological or behavioral) without accounting for broader socio-political constraints.

7.2 Practical Contributions

Beyond theory, the study offers significant implications for practitioners, policymakers, and cybersecurity professionals operating in financial services, especially in South Asia.

7.2.1. Institutional Benchmarking for Banks

The findings can act as benchmarking mechanism to the unfavorable situation of the banks in mitigating their identity theft. By doing a self-assessment of their current posture in relation to what is done by Bank A, B, and C, institutions may gauge where they stand in the technological and risk culture spectrum and strategically upgrade themselves.

7.2.2. Tailored Risk Management Strategies

The study suggests institutional-type differentiated models of identity risk management. To consider an example, prediction-based AI can be utilized in the infrastructure of the most developed private banks, whereas government-owned banks might need subsidized technologies and training of personnel. In their turn, Islamic banks require sanctions with ethically flexible approaches to dissatisfying the demands of Shariah. Such distinction is vital when applied in practice in various regulatory and cultural settings.

7.2.3. Guidance for Regulatory Bodies

The study gives evidence-based information to the State Bank of Pakistan (SBP) and other regulators. It favors the model of tiered regulations, which meet the minimum needs of rules with the ability to develop ethically and technologically. It also points out that there is need of a more versatile consultation of regulations, especially with the Islamic financial institutions.

7.2.4. Capacity Building and Workforce Development

These findings show clearly that there is an urgent need to develop capacity building of cybersecurity in the banks in the public sector. The applicable suggestions are the issuance of compulsory programs of training, certification encouragements and the possibilities of an exchange of talents with the banks of great volumes and those which lack. In case of Islamic banks, the special boundaries can be formed combining Shariah and cybersecurity in their tracks.

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

7.2.5. Customer Awareness Campaigns

Considering that there are noticeable gaps in customer digital literacy—primarily at Bank B and Bank C—the research recommends for a nationwide consumer digital literacy campaigns. These could be SMS based alerts, multi-lingual guides, and targeted campaigns for the most vulnerable demographics (e.g. on rural and elderly users).

7.2.6. Ethical AI Tool Development

The knowledge provided by Bank C leads to the idea of the increasing need of ethically compatible AI tools. Fintech developers can use this study as a guide to build privacy-respecting**,** consent-oriented, and explainable AI systems that align with religious or cultural expectations, opening new market segments in Islamic banking.

This research bridges a critical gap between global identity theft risk models and localized institutional realities in Pakistan. It contributes theoretically by offering new frameworks and ethical perspectives, and practically by providing actionable insights for diverse banking institutions, regulators, and technology providers. By combining grounded case analysis with strategic foresight, the study lays the foundation for more inclusive, culturally aware, and institutionally resilient identity theft risk assessment practices in the digital age.

8. Research Limitations and Future Work Recommendations

8.1 Research Limitations

While this study provides important insights into identity theft risk assessment practices within the Pakistani banking sector, several limitations must be acknowledged:

8.1.1. Limited Sample Size and Scope

This research is based on three case studies (Bank A, B, and C) representing private, public, and Islamic banking sectors. While the purposive selection of these cases ensures diversity in institutional type, the limited number may not capture the full spectrum of practices across all Pakistani banks, especially smaller microfinance or regional banks that may face different challenges.

8.1.2. Qualitative Data Constraints

The findings are based on qualitative interviews and document analysis, which, while rich in contextual detail, may not offer generalizable insights across the sector. The lack of quantitative validation—such as fraud incident rates, detection latency, or model accuracy scores—limits the ability to measure tool effectiveness across institutions.

8.1.3. Subjectivity in Interpretation

Despite efforts to ensure objectivity, thematic coding and interpretation of qualitative data may carry researcher bias. Participants' statements may also reflect socially desirable responses, especially in institutions where internal accountability is sensitive. Some interviewees may have overestimated or understated their bank's capabilities.

8.1.4. Data Access Restrictions

Access to internal policy documents, fraud detection protocols, and algorithmic decision systems was limited due to institutional confidentiality. This constrained the depth of analysis, particularly for AI model evaluation, biometric data management, and vendor technologies in use.

8.1.5. Ethical and Religious Complexity

While Bank C offered valuable insight into ethics-driven risk management, the diversity of Islamic interpretations across institutions was not explored. A broader Islamic finance perspective—including different schools of thought or Shariah boards—could offer a more nuanced understanding of religious constraints on technology use.

8.2 Future Work Recommendations

To expand upon the insights generated by this study, several directions for future research are recommended:

8.2.1. Multi-Bank Quantitative Studies

Future studies could include larger, sector-wide surveys involving multiple banks to statistically analyze identity theft trends, detection rates, and customer complaints. Such studies can complement qualitative insights with measurable indicators and support generalization of findings.

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

8.2.2. Comparative Regional Analysis
Comparing identity theft risk assessment practices across countries with similar financial and technological development—such as Bangladesh, Sri Lanka, or Indonesia—could help identify regional patterns and best practices applicable to South Asia or the broader Muslim-majority banking world.
8.2.3. Algorithm Auditing and Technical Evaluation
Further research should explore technical evaluations of fraud detection tools, AI-based identity scoring systems, and behavioral biometrics. Algorithm audits can help assess accuracy, fairness, and ethical implications, especially for banks that have adopted proprietary or third-party solutions.
8.2.4. Focus on Customer Behavior and Literacy
Future work should examine end-user behavior, digital trust, and literacy in more depth. Mixed-method studies involving customer surveys, app usage data, and digital ethnography can uncover how users perceive identity risk and how banks can tailor interventions accordingly.
8.2.5. Islamic Ethical AI Research
A growing opportunity exists to develop a new subfield of Islamic Ethical AI for Financial Services. Researchers can work with Shariah boards, scholars, and technologists to co-create models that uphold religious principles while enhancing fraud detection capabilities. Design frameworks, fatwa reviews, and experimental tools could all be part of this agenda.
8.2.6. Policy Impact Studies
There is a need for longitudinal policy analysis to evaluate how SBP cybersecurity guidelines, fintech laws, and data protection regulations have influenced institutional behavior over time. This can inform future regulatory design and identify areas where enforcement or support mechanisms need to be strengthened.
8.2.7. Role of Fintech and Third-Party Vendors
As banks increasingly rely on third-party technology vendors, future studies should examine vendor selection processes, data-sharing agreements, and risk outsourcing. Understanding these dynamics can offer insights into supply chain vulnerabilities in identity risk management.

Although this study offers an in-depth, multi-dimensional view of identity theft risk assessment in Pakistan's banking sector, it is limited in scale, methodology, and technical depth. Future research can build on these findings by expanding the sample size, introducing quantitative methods, and deepening exploration into ethical, cultural, and algorithmic dimensions. The fast-evolving nature of cyber threats and the rise of digital banking make this a critical area for sustained academic, technical, and regulatory engagement.

9. Conclusion

This study explored the current practices, challenges, and institutional variations in identity theft risk assessment tools within the banking sector of Pakistan through an in-depth, qualitative analysis of three banks representing private, public, and Islamic financial institutions. The research revealed stark contrasts in technological readiness, organizational culture, ethical frameworks, and regulatory interpretation. The most technologically advanced was the Bank A where AI-powered risk engines and behavioral analytics were used by the bank as a part of a proactive and innovation-driven environment. Bank B on the contrary, had major issues, such as old fashioned systems, insufficient talents and the compliance culture overriding operational culture making it difficult to curb identity thefts effectively. Bank C has trodden a different path where the risk management consideration has to be balanced with the ethical and religious considerations where the use of some technology is limited especially those that profile and deal with intrusive snooping.
These results help confirm the hypothesis that the issue of identity theft within the banking system is not only a technological one but a complicated issue on the institutional level that strongly depends on governance, ethics, capacity, and user interactions. A singular, rigid model of identity risk assessment is thus unlikely to succeed across all bank types in Pakistan. Instead, the study underscores the need for contextualized, flexible, and ethically adaptive frameworks that

Corresponding Author*: **Amna Abro**

JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

address specific institutional strengths and constraints.

Furthermore, the study contributes to both academic literature and practical implementation by highlighting localized risk cultures, uncovering under-explored ethical dimensions of identity verification, and offering a cross-case comparative framework. The importance of human capital, regulatory clarity, and customer education emerges as critical across all cases.

9.1. Policy and Practice Recommendations

Based on the study's findings and discussion, the following actionable recommendations are proposed:

9.1.1. Implement a Tiered Risk Management Framework

SBP and other stakeholders should recognize institutional diversity and support a tiered implementation strategy:

- Tier 1 (High-tech private banks): Promote innovation, AI experimentation, and ethical audits.
- Tier 2 (Islamic banks): Develop Shariah-compliant, explainable AI tools with transparent consent and use policies.
- Tier 3 (Public banks): Provide government-supported funding for core digital infrastructure and basic biometric integration.

9.1.2. Promote Cybersecurity Workforce Development

Banks, especially in the public and religious sectors, must invest in specialized training for cybersecurity and fraud detection. Cross-institutional training initiatives, regulatory certifications, and public-private partnerships can support this goal.

9.1.3. Develop Ethical AI Standards for Financial Institutions

SBP, in consultation with Islamic finance scholars, data ethicists, and technologists, should establish guidelines for ethical AI in financial services, ensuring that tools used for identity verification are transparent, fair, and aligned with local cultural norms.

9.1.4. Launch Customer Awareness Campaigns

Customer behavior is often the weakest link in identity theft. Banks should coordinate with regulators to deliver nationwide multilingual campaigns, targeting vulnerable groups through SMS, media, and on-app education.

9.1.5. Strengthen Interbank Collaboration

Banks with mature systems, such as Bank A, should be incentivized to mentor or partner with lower-capacity institutions, enabling the sharing of threat intelligence, technical assistance, and operational best practices.

9.1.6. Regularize Technical Audits and Algorithm Transparency

Regulatory bodies should enforce periodic audits of fraud detection tools and insist on algorithmic transparency to mitigate risks of bias, false positives, or breaches of customer trust.

9.1.7. Support Local Innovation in Fintech

Pakistan's growing fintech ecosystem should be leveraged to develop indigenous identity verification tools, particularly ones that integrate biometric verification with ethical, privacy-preserving machine learning techniques.

Identity theft remains a formidable threat in the evolving landscape of digital finance. While global solutions offer foundational blueprints, countries like Pakistan require locally informed, institutionally appropriate, and ethically responsible models. The success of identity risk mitigation lies not just in technological sophistication but in institutional alignment, user engagement, and cultural coherence. This study lays the groundwork for more inclusive, adaptive, and responsible identity theft prevention strategies in Pakistani banking. It is hoped that researchers, practitioners, and policymakers will continue to build on these insights to shape a secure and equitable digital banking future.

References

1. Abbas, T., & Arif, K. (2022). *Cybercrime Impact on E-Banking Adoption in Pakistan*. JISRC.
2. Abiola, O., & Salawu, R. (2023). *AI for Fraud Detection in Financial Systems*. FinTech Review.
3. Akram, H., Abdelrady, A. H., Al-Adwan, A. S., & Ramzan, M. (2022). Teachers' perceptions of technology integration in

Corresponding Author*: **Amna Abro**

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718

VOLUME . 4 ISSUE . 2 (2025)

teaching-learning practices: A systematic review. *Frontiers in psychology*, *13*, 920317.

4. Akram, H., Aslam, S., Saleem, A., & Parveen, K. (2021a). The challenges of online teaching in COVID-19 pandemic: a case study of public universities in Karachi, Pakistan. *Journal of Information Technology Education Research*, *20*, 263.
5. Akram, H., Yingxiu, Y., Al-Adwan, A. S., & Alkhalifah, A. (2021b). Technology Integration in Higher Education During COVID-19: An Assessment of Online Teaching Competencies Through Technological Pedagogical Content Knowledge Model. *Frontiers in Psychology*, 12, 736522-736522.
6. Akram, H., Yingxiu, Y., Aslam, S., & Umar, M. (2021c, June). Analysis of synchronous and asynchronous approaches in students' online learning satisfaction during Covid-19 pandemic. In *2021 IEEE International Conference on Educational Technology (ICET)* (pp. 203-207). IEEE. https://doi.org/10.1109/ICET52293.2021.9563183
7. Al-Adwan, A. S., Nofal, M., Akram, H., Albelbisi, N. A., & Al-Okaily, M. (2022). Towards a sustainable adoption of e- learning systems: The role of self-directed learning. *Journal of Information Technology Education: Re-search*, *21*, 245-267.
8. Anderson, R. et al. (2021). *Identity Theft in the Digital Age*. Journal of Cyber Risk.
9. Business Recorder. (2024). *UBL, Meezan Bank Lead in Behavioral Biometrics Pilots.*
10. Chen, Z., & Ramzan, M. (2024). Analyzing the role of Facebook-based e-portfolio on motivation and performance in English as a second language learning. *International Journal of English Language and Literature Studies*, *13*(2), 123-138.
11. Iqbal, F. et al. (2024). *Cybersecurity Practices in Pakistan's Banking Sector*. JCBI.
12. Khan, R., & Farooq, U. (2023). *Behavioral Biometrics and Digital Security in South Asia.* IJFS.
13. Ma, D., Akram, H., & Chen, I. H. (2024). Artificial Intelligence in Higher Education: A Cross-Cultural Examination of Students' Behavioral Intentions and Attitudes. *The International Review of Research in Open and Distributed Learning*, *25*(3), 134-157.
14. Ramzan, M., Akram, H., & kynat Javaid, Z. (2025). Challenges and Psychological Influences in Teaching English as a Medium of Instruction in Pakistani Institutions. *Social Science Review Archives*, *3*(1), 370-379.
15. Ramzan, M., Bibi, R., & Khunsa, N. (2023). Unraveling the Link between Social Media Usage and Academic Achievement among ESL Learners: A Quantitative Analysis. *Global. Educational Studies Review, 8*, 407-421.
16. Rehman, M. et al. (2023). *Biometric Tools in Pakistani Banks*. PJD Finance.
17. SBP. (2023). *Cybersecurity Framework for Banks.*
18. Smith, L., & Lacey, A. (2022). *Identity Fraud Risk Models in Online Banking.* Journal of Financial Cybersecurity.
19. Zhao, D., & Lee, J. (2021). *Machine Learning for Identity Theft Detection*. IEEE FinTech.
20. Govindarajan, V., & Muzamal, J. H. (2025). Advanced cloud intrusion detection framework using graph based features transformers and contrastive learning. Scientific Reports, 15(1), 20511. https://doi.org/10.1038/s41598-025-07956-w
21. Govindrajan, V. (2025, March). Machine learning based approach for handling imbalanced data for intrusion detection in the cloud environment. In 2025 3rd International Conference on Disruptive Technologies (ICDT) (pp. 810-815). IEEE. https://doi.org/10.1109/ICDT63985.2025.1098661

Corresponding Author*: **Amna Abro**